

---

**DAY 14: Bitcoin Self Custody**

1 message

**21 Days of Bitcoin**

Tue, Aug 30, 2022 at 11:08

&lt;education@bitcoinmagazine.com&gt;

PM

Reply-To: 21 Days of Bitcoin &lt;education@bitcoinmagazine.com&gt;

To: samglaj3p@gmail.com



Today is the day you learn about self-custody. This is a challenging process that takes time to learn and is a daunting next-step to take. However, continue to ask questions (tweet them with **#21DaysofBitcoin** for help!) and do the necessary research, because self-custody is the entire purpose of owning bitcoin.

---

## ***Why Self Custody?***

Yesterday, we went over buying bitcoin from exchanges. However, the bitcoin you're currently keeping on Coinbase isn't technically "yours" yet. If someone hacks your Coinbase account (or Coinbase itself), there would be no way to recover your funds or trace who did the crime.

Even if you're not worried about hackers, it is in the bitcoin ethos to strive for self-sovereignty; after all, if the government can access and seize your bitcoin because it's on a *centralized* exchange, doesn't that defeat the purpose of this *decentralized* asset?

## ***What does it mean to "own" your bitcoin?***

In order to truly own and protect your bitcoin, you will need to have your own set of "private keys" that only you have access to, unlike the publicly shared invoice address that you use to receive bitcoin with.

## ***Private Keys Explained***

Private keys are essentially very complex, randomly-generated passwords that allow us to access our bitcoin and to verify or "sign" our transactions. These keys are then represented in a 12 or 24-word "seed phrase," which allows us to more easily record, memorize, and backup our private keys.

# Private Key

**Hex:** DD5113FEDED638E5500E65779613BDD3BDD8EB8E5D86CDD3370E629B02E92CD


**Base64:** 3VET/r7WOOVQDmV3lhO9073b64612GzdM3DmKbAuks0=

**WIF:** 5KVkpWGFdQGjAUeEDUFbrFwxNPjmXy5kBBmRzzBDf4JkgFXqXTa

**Binary:**  
110111010101000100010011111111011011101101101010100011100011100101010100  
0000001110011001010111011110010110000100111011101101000111011101101  
1011110101110001110101101011011000011011001101110100110011011000011  
1001100010100110110000001011101001001011001101

Seed phrase example:  
1)cheese 2)wine 3)butter 4)egg 5)muffin 6)banana  
7)pizza 8)cream 9)milk 10)noodle 11)sugar 12)rice

written in different formats



On an exchange like Coinbase, your bitcoin is stored in a “hot wallet,” where Coinbase owns your private keys. Because they own your keys, if they get hacked, so does everyone who keeps their bitcoin on there — yikes.

Only when you have control of your private keys will you have secure control over your bitcoin transactions.

Keep in mind though, that self-custody means you’re responsible for keeping these seed phrases offline and in a safe place where you won’t lose access to them. While there are methods of backing up your seeds onto physical, stainless steel cards, it’s not as easy as storing it in an online password manager.

Many of us have heard the woes of those who lost access to or forgot their seed phrases, thus losing access to millions of dollars worth of bitcoin. Let this be a lesson to us all: *Keep your seeds safe, secure, and accessible.*

---

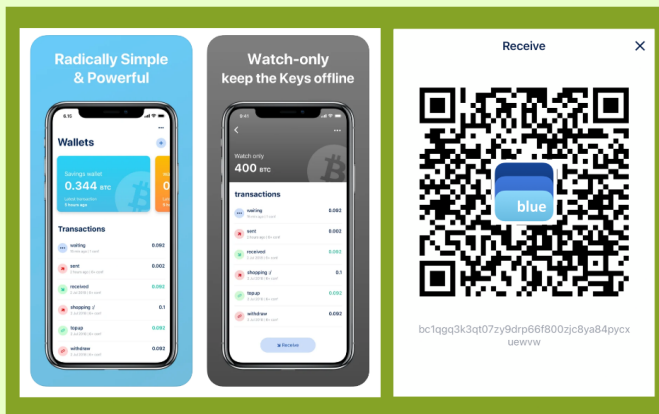
## ***Easy Self Custody Methods***

In this lesson, I’ll introduce two easy forms of bitcoin storage methods so that you can begin your self-custody journey:

### **1. Software wallets**

There are a few open source mobile options out there that are great starting points for beginners, such as Blue Wallet and Muun Wallet. Desktop versions like Electrum are also an option.

# Software Wallet



Although these wallets are connected to the internet, they generate a new private key that only you can control, which is a big step up from exchange-hosted wallets.

The great thing about having mobile/desktop wallets is that you can easily access your bitcoin anytime. The downside is that if you don't take the right security measures, someone who has access to your phone or computer could also have access to your online bitcoin wallet.

While mobile wallets are good for on-the-go use, they're not the most secure. If you are just starting out with minimal funds, software wallets are a great, free option.

Fortunately, there are also more advanced options to utilize your software wallets as “watch only” wallets, where they merely act as a user interface for your cold storage but do *not* hold your private keys. This would allow you to generate invoice addresses for receiving bitcoin, but would prevent a hacker from transferring anything out.

## 2. Hardware wallets

Hardware wallets are the most straightforward and popular form of offline cold storage. These wallets securely contain your private keys and typically come in the form of a flash drive-like device (popular ones include the Ledger Nano S or the Coldcard). The devices themselves are protected with a PIN so that your private key will still be somewhat safe even if your hardware wallet is stolen.



Because your hardware is not connected to the internet, it is considered “cold” and a much safer method of private key storage than online “hot” wallets. These physical devices allow you to access your bitcoin securely by storing your private keys offline.

It’s a common misconception to think that your hardware wallets “hold” your bitcoin — your bitcoin lives on the blockchain; the hardware wallet is merely a means of storing and using your private key to authorize transactions that move funds. Although a hacker could guess your pin to access your hardware wallet, it is extremely unlikely as most wallets will wipe themselves out after a few wrong guesses.

If this physical device is lost or stolen, you can still recover your funds with a new hardware or software wallet, as long as you have access to

your seed phrase.

## ***Additional Security Measures***

With great power comes great responsibility, and the ability to self-custody your bitcoin is a great power indeed. Aside from removing your bitcoin off of exchanges, making sure your seed phrases are kept private and secure is of utmost importance — this is your only backup.

Many people like to take on additional security measures by storing backups of their seed phrases in vaults, or setting up more advanced [multi-signature wallets](#) that require additional private keys to authorize transactions.

On another note, be aware of phishing scams like fake hardware wallets being sold by scammers on Amazon or Ebay; always purchase directly from the manufacturer to ensure that your hardware wallet is the real deal.

It's time to take your first step in bitcoin self-custody.

And, remember, *not your* 🗝️, *not your* 💰.

**#21DaysofBitcoin**



## **Bitcoin Magazine PRO**

**Save 40%** on your first year subscription with Bitcoin Magazine PRO. Insights on bitcoin markets, global macro, & in-depth research reports published monthly.

**[Take 40% off](#)**

## Bitcoin Magazine Print

Take **\$12 off** your annual print subscription. Get 4 issues/year to your mailbox, starting with The Censorship Resistant Issue.

Promo code: **"21DAYS"**



## Bitcoin Magazine Store

Take **21% off** our collection of bitcoin shirts, hats, or mugs from the official Bitcoin Magazine store.

Promo code: **"STORE21D"**



*Copyright © 2022 BTC Media, All rights reserved.*

You are receiving this email because you opted in via our web page.

**Want to change how you receive these emails?**

You can update your preferences or unsubscribe from this list.

[Terms & Conditions](#) • [View email in browser](#)

